International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR)
ISSN(P): 2249-6831; ISSN(E): 2249-7943
Vol. 5, Issue 4, Aug 2015, 1-8
TJPRC Pvt. Ltd.

FIGHTING CYBERCRIME: A COMPARISON OF THE CYBERCRIME LAWS IN SAUDI ARABIA AND THE UNITED STATES

ABDULLAH ALMUQRIN, KONNIE KUSTRON, JD

College of Technology, Eastern Michigan University, United States

ABSTRACT

The benefits of the internet are numerous especially with the continuous development in technology. Unfortunately, these benefits come with a price. Cybercrime is increasing and expanding day after another. Attackers come from different countries and they are able to cripple the economy in different ways. Many countries realized this danger and enacted cybercrime laws to fight this type of crimes. This study introduces a comparison between cybercrime law in the United States and in Saudi Arabia. Both laws aim towards reducing and eliminating cybercrime by punishing the attackers

KEYWORDS: Cybercrime, Laws, Security

INTRODUCTION

The Internet was not popular in the 1980s and early 1990s and only was limited to some academic and scientific institutions. The Internet became commonly accepted in the middle of the 1990s and this growth was associated with the introduction of the intranet and computer networks in many businesses (Thompson, 2014). It was estimated that Internet users in 2014 have reached about 3 billion from countries around the world with China and the United States on top of these countries (Internet Users, 2014). China represents 22% of all Internet users and is ranked first and the United States represents 10% of Internet users and is ranked second, while Saudi Arabia is ranked 30th representing 0.6% of the world Internet users (Internet Users, 2014). The number of internet users depends mainly on the number of population in each country (Internet Users, 2014)

In this period too, cybercrime expanded from just some individual hacking cases for enjoyment to organized and more complicated groups that have the skills and expertise to attack vigorously crippling their targets. Not all countries have cybercrime laws or consider law enforcement for cybercrimes that gives the chance to many cyber-attacks to be directed from these countries (Thompson, 2014). Attackers are simply free to launch their cybercrimes from Russia or China and feel safe knowing that law enforcement is absent and no one can stop them (Bradbury, 2012). Cybercrime became a business that uses technology in committing effective and unprecedented crimes. The scale and the effect of these crimes are profound and cannot be attained in the physical world. There are very distinct cybercrimes such as the 253 data breaches reported in 2014 allowing the exposure of more than 552 million identities (Thompson, 2014, p. 2). The United States and Saudi Arabia are from the countries that have cybercrime laws and penalties, but cybercrime laws have to be enforced globally to be more effective on a larger scale (Thompson, 2014).

Cases of Cyber-Attacks in the United States

There are many cases of cybercrimes that affect businesses and even the government in the United States.

The following cybercrime cases are considered the worst:

- The White House was a target to a cyber-intrusion in October 2014. This attack is under investigation from the FBI and other US intelligence agencies. It is believed that the Russian government hired these attackers to make this serious and sophisticated intrusion on the U.S. government, but this information is not verified yet (Perez, &Prokupecz, 2015).
- The attack of November 2013 on Target Corporation targeted customer's credit and debit card numbers and other confidential information. The hackers who were from Russia, were able to obtain this information and managed to upload the data of 110 million customers to an external server without detection (Kadivar, 2014).
- The attack on Google that started in June 2009 was committed by a Chinese corporation specialized in cyber-espionage called Elder wood Gang. Attackers gained access to Google's source code repositories using a complex technique and were able to extract sensitive data about Google's business without detection (Kadivar, 2014).
- The attack on the New York Times in October 2012 was committed by techniques used by the Chinese military. The hackers targeted data of the New York Times' employees and reporters along with their passwords. The purpose of this attack was to get hold of the names of those who assisted in obtaining information about the relatives of the Chinese prime minister. Accordingly the data of 50 employees and reporters were uploaded to an external server (Kadivar, 2014).
- The attack of May 2006 on TJX Corporation was carried by an unknown criminal group who was able to obtain the numbers of credit and debit cards of more than 94 million customers. The hackers were able to upload this information to an external server and were not detected (Kadivar, 2014).

Cases of Cyber-Attacks in Saudi Arabia

Saudi Arabia was also targeted by hackers and some of the worst cyber-attacks in Saudi Arabia are:

- The attack on Aramco Company in August 2012. Aramco is one of the well-known oil companies owned by the Saudi Arabian government. In this incident, 30,000 computers at this company were attacked by a virus leading to data destruction and the deletion of data on the company's hard-drives. It was believed that the purpose of this attack is to interrupt the production of oil in the company (Elnaim, 2013).
- Multiple attacks from outside the country targeted Saudi Arabia's government websites, crippling these websites for quite some time until they were disabled (Elnaim, 2013). It was said that these attacks were discovered to belong to hundreds of IP addresses from different parts of the world (Reuters, 2013).
- The 2012 attack on King Saud University, a public university established in Riyadh, Saudi Arabia. The university was subject to the exposure of its database which included 812 users. The data that included phone numbers, addresses, and passwords was hacked from the university website and disclosed on the internet on a file sharing site (Elnaim, 2013).
- In May 2013, the computers of the national police were targeted by hackers leading to their crash after accepting a massive amounts of service requests (Reuters, 2013).

- In May 2013 also, the Financial Times newspaper's website and Twitter feed in Saudi Arabia were exposed to cyber-attacks believed to be from a group of activists who support the Syrian president and its army (Reuters, 2013).

Challenges of Cybercrime

While crimes have different types and shapes, cybercrime is an internet-based crime using a computer and network. Cybercrime includes a wide range of unlawful acts such as data theft, copyright infringement, identity theft, and dissemination of computer viruses and malware, fraud, and many other criminal activities (Hu, Chen, & Bose, 2013). Cybercrime is exponentially rising with the continuous development of technology in computers and mobile phones. Cybercrime became easier when most of individuals and businesses have switched to online transactions (Broadhurst, 2006). With more online traffic, the possibility of illegal activities increased.

Criminals create new methods to commit their crimes using the internet and modern technology. Cyberspace perpetrators cannot be easily identified since they can be of any age and nationality. They can be individuals, disciplined groups, or whole states. Victims of cybercrimes are internet users from different ages and nationalities. They can be individuals, organizations, and governments (Desnoyers, 2013). Cybercrime is a growing threat affecting the digital world and everyone using it. Fighting cybercrime has come to be a common goal for many countries around the world to avoid information security breaches (Hu, Chen, & Bose, 2013).

The United States and Saudi Arabia are two of the countries that recognized the importance of enacting laws to face the globalized cybercrime and punish its perpetrators. The economic costs of cybercrimes in both the United States and Saudi Arabia is staggering. In 2014, it was estimated that cybercrime approximately cost the United States around $100 billion a year (Kopan, 2014). However, the cost of cybercrime in Saudi Arabia exceeds $1.9 billion a year (Almerdas, 2014). Both the United States and Saudi Arabia have their own separate anti-cybercrime laws that address the most prevailing crimes in each country.

Cybercrime Law in the United States

In the United States, the Computer Fraud and Abuse Act (CFAA) was enacted by the Congress in 1986 as a separate and new statute, 18 U.S.C. § 1030 to address computer related crimes. The congress continued to revise federal criminal laws and make the suitable amendments to address the evolving crimes associated with computer and internet use. Examples of these amendments are: the change made to 18 U.S.C. § 1030(a)(2)(C) to eliminate the concept that stealing information involves "interstate or foreign communication, thereby expanding jurisdiction for cases involving theft of information from computers" and also the change made to 18 U.S.C. § 1030(a)(5) to stop eliminating the effect of the defendant's action to just a loss exceeding $5,000 to "a felony offense where the damage affects ten or more computers" (Jarrett, &Bailie 2010, p. 2). The CFAA set penalties on cybercriminals and held them liable for the infringements they impose on people and government (McCormick, 2013). The CFAA safeguarded computers from being subject to trespassing, threats, damage, espionage, and from being corruptly used as instruments of fraud (§ 1030).

Legal System in Saudi Arabia

Saudi Arabia is an Islamic state that takes the Islamic law (Shari'ah) the base for its legal and judicial system.

Islamic law is used for civil cases as well as criminal ones. The King of Saudi Arabia is the head of the legal system. The king represents the final court of appeal and in his hands the power of pardon. The Saudi court system consists of three fundamental branches: the Shari'ah Courts, the Board of Grievances, and various committees within government ministries (Legal and Judicial Structure, 2015).

In Saudi Arabia, the Shari'ah or Islamic Law is considered the directory and guide for all legal issues and it is applied on both sacred and secular issues (Legal and Judicial Structure, 2015). **According to Shari ah the defendant is innocent until proven guilty and severe punishment is only applied for dangerous or repeated crimes. There are four sources for the derivation of the Shari'ah law. The main source of Shari'ah law is the** Holy Qur'an and comes next the "Sunnah" (Legal and Judicial Structure, 2015). The "Sunnah" is Prophet Muhammad's sayings and practices applied throughout his life (Legal and Judicial Structure, 2015). In the third place comes the "Ijma'", which is the agreement of viewpoint of Muslim scholars on the principles and standards concerning a specific case that took place after the death of the Prophet (Legal and Judicial Structure, 2015). In the fourth place comes the "Qias" or analogy (Legal and Judicial Structure, 2015)

Cybercrime Law in Saudi Arabia

Saudi Arabia is the most targeted country for cybercrime in the Persian Gulf region. Computer and internet users know about cybercrime, but they are less aware of the legislations counteracting these crimes (Elnaim, 2013). Saudi Arabia has its own anti-cybercrime law that punishes cyberspace offenders.

Table (1) shows a comparison between cybercrime laws in the United States and Saudi Arabia and the penalties associated with each one of them.

Table 1: Comparison of Cybercrime Laws in the United States and Saudi Arabia

Crime	Penalty in USA	Penalty in Saudi Arabia
Computer espionage and abuse	Usually imprisonment not more than 10 years, but may reach 20 years for repeated convictions, and/or a fine under Title 18, 18 U.S.C. 1030(c)(1)	Usually imprisonment not more than ten years and/or a fine of $1.3 million (Article 7)
Obtaining information by unauthorized computer access	Imprisonment can be from one year to five years or can reach ten years depending on whether the offence was simple or repeated and/or a fine under Title 18, 18 U.S.C. 1030(c).	Usually imprisonment not more than a year and/or a fine of $130,000 (Article 3)
Trespassing in government cyberspace	Imprisonment is usually one year and can reach ten years for repeated offences and/or a fine under Title 18. The fine can reach $100,000 for misdemeanors and $250,000 for felonies or can be calculated to be double the loss or gain resulted from this crime according to 18 U.S.C. 1030(a)(3)	Usually imprisonment not more than ten years and/or a fine of $1.3 million (Article 7)
Computer fraud	Usually imprisonment is not more than five years, but can reach ten years for repeated convictions. A fine under Title 18, 18 U.S.C. 1030(c)(4) can be titled with or without Imprisonment, and under 18 U.S.C. 1030(g), victims can be compensated for damages and/or sue for injunctive relief. Other federal laws can be applied for different types of fraud such as 18 U.S.C. 1343 for wire fraud, 18 U.S.C. 1832 for	Usually imprisonment not more than three years and/or a fine of $520,000 (Article 4)

	theft of trade secrets, 18 U.S.C. 2319 for copyright infringement, and 18 U.S.C. 1029 for fraud involving credit cards and device access	
Causing computer damage There are three elements of the damage here, "A) intentionally causing unauthorized damage by knowingly causing a transmission to a protected computer; (B) recklessly causing damage by intentionally accessing a protected computer; or (C) negligently causing damage and loss by intentionally accessing a protected computer" (18 U.S.C. 1030(a)(5)).	For the first element (a)(5)(A), the criminal is imprisoned from one to ten years and it can reach twenty years for repeated convictions. For the second element (a)(5)(B), the criminal is punished by imprisonment from one to five years and it can reach twenty years for repeated offence. For the third element (a)(5)(C), the offender is imprisoned for not more than one year and can reach ten years for repeated offence	Usually imprisonment not more than a year and/or a fine of $130,000 (Article 3)
Trafficking in computer access	Usually imprisonment for not more than one year and/or a fine under Title 18, 18 U.S.C. 1030(c)(2). For repeated offenses, the imprisonment can reach ten years and criminals are held liable to victims under 18 U.S.C 1030(g)	Usually imprisonment not more than four years and/or a fine of $800,000 (Article 5)
Extortionate threats	Usually imprisonment for not more than five years and/or fine under Title 18, 18 U.S.C. 1030(c). For repeated offenses, imprisonment can reach ten years and victims can be compensated for damages under 18 U.S.C. 1030(g)	
The production and dissemination of programs that violate discipline, ethics and Islamic values, or promote pornography, drug use, or gambling (Article 6)		Usually imprisonment not more than five years and/or a fine of $800,000 (Article 6)

DISCUSSIONS

The internet became part of the society's everyday life, but it brought about new vulnerabilities such as cybercrimes. Many countries recognized these vulnerabilities and tried to protect itself by taking the required precautions and enacting cybercrime laws. The United States and Saudi Arabia are two of these countries that took cybercrime seriously and enacted cybercrime laws to protect its people from these crimes.

In the United States, the Computer Fraud and Abuse Act (CFAA) was enacted by the Congress in 1986 as a separate and new statute, 18 U.S.C. § 1030 to address computer related crimes. In Saudi Arabia a cybercrime law was also enacted. Both laws were divided into sections where each section includes the offence and the punishment associated with this offence. In both laws, the punishment is imprisonment and/or a fine. The punishment depended on the type of crime only in Saudi Arabia, while in the United States the punishment depended too on whether the crime was done for the first time or was repeated more than once.

CONCLUSIONS

Cybercrimes are a new challenge to the whole world and laws are required to be enforced in every country using the internet. It is clear that cybercrimes has maximized dramatically and they can affect people, governments, and

businesses deeply. Enacting cybercrime laws is considered the first line of defense on the internet. Fighting cybercrime should be the common goal to avoid information security breaches that affect almost everyone. For cybercrime laws to be effective, people have to be aware of these laws and know how to protect their information online by taking the adequate precautions.

REFERENCES

1. Anti-cybercrime Law. (2010). Anti-cybercrime law. *Saudi Embassy*. Retrieved from http://www.saudiembassy.net/announcement/announcement03260701.aspx
2. Almerdas, S. (2014). The criminalization of identity theft under the Saudi anti-cybercrime law 2007. Journal of International Commercial Law and Technology, 9(2), 80-93.
3. Arab News. (2012). Cybercrime costs Saudi Arabia SR 2.6 bn. a year. *Arab News.*
4. Bradbury, D. (2012). When borders collide: Legislating against cybercrime. *Computer Fraud & Security, 2012*(2), 11-16.
5. Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime. *Policing, 29*(3), 408-433.
6. Computer Fraud and Abuse Act (CFAA)18 U.S.C. § 1030
7. Desnoyers, S. (2013). *The challenges of cybercrime for international law enforcement* (Order No. 1551187). Available from ProQuest Dissertations & Theses Global. (1498133652).
8. Elnaim, B. M. (2013). Cyber Crime in Kingdom of Saudi Arabia: The Threat Todayand the Expected Future. Information and Knowledge Management, 3(12), 14-19
9. Hu, Y., Chen, X., & Bose, I. (2013). Cybercrime enforcement around the globe. *Journal of Information Privacy & Security, 9*(3), 34-52.
10. Internet Users. (2014). Internet users. *Internet Live Stats.* Retrieved from http://www.internetlivestats.com/internet-users/
11. Jarrett, H. M., &Bailie, M. W. (2010). Prosecuting Computer Crimes: Computer Crime and Intellectual Property Section Criminal Division. *Office of Legal Education Executive Office for United States Attorneys,* 1-207. Retrieved from http://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf
12. Jewkes, Y., &Yar, M. (2010). *Handbook of Internet Crime*. Cullompton, Devon: Willan Publishing
13. Legal and Judicial Structure. (2015). Legal and judicial structure. Saudi Embassy. Retrieved from http://www.saudiembassy.net/about/country-information/government/legal_and_judicial_structure.aspx
14. Kadivar, M. (2014). Cyber-attack attributes. *Technology Innovation Management Review, 4*(11), 22-27.
15. Kopan, T. (2014). Cybercrime costs $575 billion a year, $100 billion to US. *Politico.* Retrieved fromhttp://www.politico.com/story/2014/06/cybercrime-yearly-costs-107601.html
16. McCormick, W. C. (2013). The computer fraud and abuse act: Failing to evolve with the digital age. *SMU Science and Technology Law Review, 16*(3), 481.

17. Norton. (2012). 2012 Norton Cybercrime Report. *Symantec*. Retrieved from http://nowtatic.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf
18. Perez, E., &Prokupecz, S. (2015). How the U.S. thinks Russians hacked the White House. CNN. Retrieved from http://www.cnn.com/2015/04/07/politics/how-russians-hacked-the-wh/
19. Reuters. (2013). Saudi Arabia faces major cyber attack. *Gulf News.* Retrieved from http://gulfnews.com/news/gulf/saudi-arabia/saudi-arabia-faces-major-cyber-attack-1.1184977
20. Thompson, L. (2014). *Defending against cybercrime* (Order No. 1570878). Available from ProQuest Dissertations & Theses Global. (1640916948).